

**COMMERCIALLY HOSTED INFRARED  
PAYLOAD (CHIRP)**

**DD FORM 254 CONTRACT SECURITY  
CLASSIFICATION SPECIFICATION**

**ATTACHMENT 4  
To  
CONTRACT**

**FA8814-08-C-0001**

**19 June 2008**

<b>DEPARTMENT OF DEFENSE</b> <b>CONTRACT SECURITY CLASSIFICATION SPECIFICATION</b> <i>(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)</i>				<b>1. CLEARANCE AND SAFEGUARDING</b> a. FACILITY CLEARANCE REQUIRED Top Secret b. LEVEL OF SAFEGUARDING REQUIRED Top Secret																																																																																																																	
<b>2. THIS SPECIFICATION IS FOR: (X and complete as applicable)</b> <input checked="" type="checkbox"/> a. PRIME CONTRACT NUMBER FA8814-08-C-0001 <input type="checkbox"/> b. SUBCONTRACT NUMBER <input type="checkbox"/> c. SOLICITATION OR OTHER NUMBER      Due Date (YYMMDD)			<b>3. THIS SPECIFICATION IS: (X and complete as applicable)</b> <input checked="" type="checkbox"/> a. ORIGINAL (Complete date in all cases)      Date (YYMMDD) 080619 <input type="checkbox"/> b. REVISED (Supersedes all previous specs)      Revision No.      Date (YYMMDD) <input type="checkbox"/> c. FINAL (Complete Item 5 in all cases)      Date (YYMMDD)																																																																																																																		
<b>4. IS THIS A FOLLOW-ON CONTRACT?</b> <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract																																																																																																																					
<b>5. IS THIS A FINAL DD FORM 254?</b> <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes complete the following In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.																																																																																																																					
<b>6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)</b> a. NAME, ADDRESS, AND ZIP CODE      b. CAGE CODE      c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Americom Government Services      [REDACTED]      Defense Security Service Ind. Sec. Field Office (SIIML) [REDACTED]      307 Fellowship Road, Suite 115 Mt. Laurel, New Jersey 08054-1233																																																																																																																					
<b>7. SUBCONTRACTOR</b> a. NAME, ADDRESS, AND ZIP CODE																																																																																																																					
<b>8. ACTUAL PERFORMANCE</b> a. LOCATION      b. CAGE CODE      c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) See performance locations in attachment																																																																																																																					
<b>9. GENERAL IDENTIFICATION OF THIS PROCUREMENT</b> 3 <sup>rd</sup> Generation IR Surveillance (3GIRS) Commercially Hosted Infrared Payload (CHIRP)																																																																																																																					
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2"><b>10. THIS CONTRACT WILL REQUIRE ACCESS TO:</b></td> <td>YES</td> <td>NO</td> <td colspan="2"><b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b></td> <td>YES</td> <td>NO</td> </tr> <tr> <td>a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td>a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY</td> <td></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>b. RESTRICTED DATA</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td>b. RECEIVE CLASSIFIED DOCUMENTS ONLY</td> <td></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION</td> <td></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>c. RECEIVE AND GENERATE CLASSIFIED MATERIAL</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>d. FORMERLY RESTRICTED DATA</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td>d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>e. INTELLIGENCE INFORMATION:</td> <td></td> <td></td> <td></td> <td>e. PERFORM SERVICES ONLY</td> <td></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>  (1) Sensitive Compartmented Information (SCI)</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td>f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>  (2) Non-SCI</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td>g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>f. SPECIAL ACCESS INFORMATION</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td>h. REQUIRE A COMSEC ACCOUNT</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>g. NATO INFORMATION</td> <td></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>i. HAVE A TEMPEST REQUIREMENT</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>h. FOREIGN GOVERNMENT INFORMATION</td> <td></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>i. LIMITED DISSEMINATION INFORMATION</td> <td></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>j. FOR OFFICIAL USE ONLY INFORMATION</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td>l. OTHER (Specify):</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>k. OTHER (Specify) Data Dissemination</td> <td></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td>Technology Transfer and Information Control, Arms Export Control</td> <td></td> <td></td> <td></td> </tr> </table>						<b>10. THIS CONTRACT WILL REQUIRE ACCESS TO:</b>		YES	NO	<b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b>		YES	NO	a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RESTRICTED DATA		<input checked="" type="checkbox"/>	<input type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		<input checked="" type="checkbox"/>	<input type="checkbox"/>	d. FORMERLY RESTRICTED DATA		<input checked="" type="checkbox"/>	<input type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		<input checked="" type="checkbox"/>	<input type="checkbox"/>	e. INTELLIGENCE INFORMATION:				e. PERFORM SERVICES ONLY		<input type="checkbox"/>	<input checked="" type="checkbox"/>	(1) Sensitive Compartmented Information (SCI)		<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		<input checked="" type="checkbox"/>	<input type="checkbox"/>	(2) Non-SCI		<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. SPECIAL ACCESS INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT		<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. NATO INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT		<input checked="" type="checkbox"/>	<input type="checkbox"/>	h. FOREIGN GOVERNMENT INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		<input checked="" type="checkbox"/>	<input type="checkbox"/>	i. LIMITED DISSEMINATION INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<input checked="" type="checkbox"/>	<input type="checkbox"/>	j. FOR OFFICIAL USE ONLY INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER (Specify):		<input checked="" type="checkbox"/>	<input type="checkbox"/>	k. OTHER (Specify) Data Dissemination		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Technology Transfer and Information Control, Arms Export Control			
<b>10. THIS CONTRACT WILL REQUIRE ACCESS TO:</b>		YES	NO	<b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b>		YES	NO																																																																																																														
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																																																																														
b. RESTRICTED DATA		<input checked="" type="checkbox"/>	<input type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																																																																														
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																																																																														
d. FORMERLY RESTRICTED DATA		<input checked="" type="checkbox"/>	<input type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																																																																														
e. INTELLIGENCE INFORMATION:				e. PERFORM SERVICES ONLY		<input type="checkbox"/>	<input checked="" type="checkbox"/>																																																																																																														
(1) Sensitive Compartmented Information (SCI)		<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																																																																														
(2) Non-SCI		<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																																																																														
f. SPECIAL ACCESS INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT		<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																																																																														
g. NATO INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT		<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																																																																														
h. FOREIGN GOVERNMENT INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																																																																														
i. LIMITED DISSEMINATION INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																																																																														
j. FOR OFFICIAL USE ONLY INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER (Specify):		<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																																																																														
k. OTHER (Specify) Data Dissemination		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Technology Transfer and Information Control, Arms Export Control																																																																																																																	

12. PUBLIC RELEASE Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public release shall be submitted for approval prior to release



Direct



Through (Specify):

The contractor shall refer to the ALTERNATIVE INFRARED SATELLITE SYSTEM Program Protection Plan/SCG for procedures regarding the release of program information to the general public and to US citizens Release of information must be approved by SMC/PA.

To the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)\* for review.  
\*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicate a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any document/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.

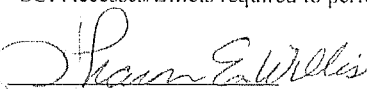
The National Industrial Security Program Operating Manual (NISPOM) dated February 2006 applies to this contract.

The contractor shall protect Critical Program Information, technologies, and systems (CPI), and Critical System Resources (CSR), as identified in the Program Protection Plan and as identified in the contractor's Program Protection Implementation Plan, as approved by the 3<sup>rd</sup> Generation Infrared Surveillance System (3GIRSS) program office. The prime contractor will flow-down applicable critical program information, technologies, and systems (CPI) and Critical System Resources (CSR) to any subcontractor with protection requirements as identified in its Program Protection Implementation Plan. Additionally, classified national security information, special access and unclassified controlled information as prescribed in applicable security classification guides will be protected as outlined in the NISPOM.

Program Manager: LtCol Eric Moltzau, SMC/XRF

Estimated Date of Completion: September 30, 2012

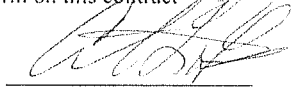
SCI Accesses/Billets required to perform on this contract



SHARON E WILLIS

Industrial Security Officer

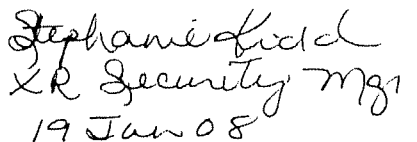
SMC/PIP 6/19/08



CALVIN L. FISHER

Deputy Director of Intelligence

SMC/INS

  
XR Security Mgr.  
19 Jan 08

See attachment for further guidance.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)



Yes



No

Contractor employees and subcontractors who have access to Air Force networks must have granted security clearance.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)



Yes



No

DSS is relieved of responsibility for SMC/XR SCI material. SMC/XR, 483 North Aviation Boulevard, El Segundo CA 90245 has exclusive security responsibility for all SAP material released or developed under this contract. See attachment #2 for guidance on SCI information. See attachment #1 for additional caveats.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

Joseph Simonds

b. TITLE

Contracting Officer

c. TELEPHONE (Include Area Code)

(310)653-9245

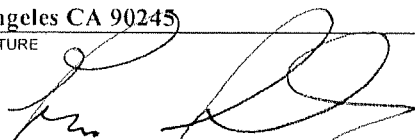
d. ADDRESS (Include ZIP Code)

483 North Aviation Blvd

SMC XRC

Los Angeles CA 90245

e. SIGNATURE



17. REQUIRED DISTRIBUTION



a. CONTRACTOR



b. SUBCONTRACTOR



c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR



d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION



e. ADMINISTRATIVE CONTRACTING OFFICER



f. OTHERS AS NECESSARY (SMC/PIP) (SMC/IN)

**ATTACHMENT TO**  
**CONTRACT NO.: FA8814-08-C-0001**

**CONTRACT SECURITY CLASSIFICATION  
SPECIFICATION (DD FORM 254)**

**FOR**

**3<sup>rd</sup> Generation IR Surveillance (3GIRS) System  
Commercially Hosted IR Payload Program**

**DATE:**  
**19 June 2008**

### Reference Block 8 a/b/c: Actual Performance

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
<p>The following facility is providing administrative function, no classified access/storage is required:</p> <p>Americom Government Services [REDACTED] [REDACTED]</p>	[REDACTED]	<p>Defense Security Service Ind. Sec. Field Office (SIIML) 307 Fellowship Road, Suite 115 Mt. Laurel, New Jersey 08054-1233</p>
<p>The following facilities below are authorized storage up to the TS.SCI level and SCI will be performed at those locations.</p>		
<p>SAIC [REDACTED] [REDACTED] [REDACTED]</p>	[REDACTED]	<p>Defense Security Service 21151 Western Avenue Torrance, CA 90501</p>
<p>SAIC [REDACTED] [REDACTED] [REDACTED]</p>	[REDACTED]	<p>Defense Security Service 11770 Bernardo Plaza Court, Suite 450 San Diego, CA 92128-2426</p>
<p>Orbital Sciences Corporation [REDACTED] [REDACTED]</p>	[REDACTED]	<p>Defense Security Service 14428 Albemarle Point Place Chantilly, VA 20151</p>

### Reference Block 10a and 11h: Communications Security (COMSEC)

1. The Contractor is authorized access to COMSEC information and will comply with National Security Agency Central Security Service NSA/CSS Policy Manual No.3-16 (replaced NSA Manual 90-1.) Access to COMSEC material/information is restricted to U.S. citizens who have been briefed according to the NISPOM and possess an approved government clearance. NOTE: The COMSEC/CRYPTO briefing applies only to the use and control of CRYPTO equipment and specialized COMSEC publications.

2. NACSIM/NACSEM documents are not considered COMSEC controlled material. Additionally, cryptographic information/equipment shall be retained in a Contractor facility COMSEC account.

### Reference Block 10b and 10d: Restricted Data And Formerly Restricted Data

The contractor is permitted access to restricted data and formerly restricted data in performance of this contract. Restricted Data and Formerly Restricted Data will be handled in accordance with appropriate security markings and handling caveats and in accordance with Chapter 9, Section 1 of the NISPOM.

## **Reference Block 10e: Intelligence Information**

### **(1) Sensitive Compartmented Information (SCI)**

#### **a. Physical Security**

This contract requires access to Sensitive Compartmented Information (SCI). The Director of Intelligence, Surveillance, and Reconnaissance / Deputy Chief of Staff, Air and Space Operations, USAF, has exclusive security responsibility for all SCI classified material released to or developed under this contract. This SCI information must be maintained in a Sensitive Compartmented Information Facility (SCIF). DCID 6/4, 6/9, DoD 5105.21-M-1 and AFMAN 14-304 serve as the necessary guidance for physical, personnel, and information security measures and are part of the security specification for this contract. Contractor compliance with these directives is mandatory unless specifically waived. Inquiries pertaining to classification guidance for SCI will be directed to SMC/INS through the Contract Monitor. The contractor is required to comply with the physical security standards as defined in DCID 6/9, DOD 5105.21-M-1 and AFMAN 14-304. SCI material released to the contractor under this contract shall be stored and worked on only within the proposed facility and upon receipt of an approved physical security accreditation by SSO DIA/DAC. AFSPC sponsored SCIF shall not be co-utilized with other government agencies unless covered by an approved Co-Utilization Agreement (CUA). The User Agency SSO is SMC/INS, Los Angeles AFB, CA. Work performed under this contract shall not be accomplished in a SCIF accredited by another Government Organization unless there is an approved CUA between that organization and SMC/INS. Applicable Program Security Classification guidance will be identified in block 13 of this DD Form 254.

#### **b. Personnel Security**

The contractor shall nominate a CSSO and Alternate to SMC/INS. No contractor will be granted access to SCI information/material under this contract unless they are filling a SMC/IN SCI billet assigned under this contract. The names of contractor personnel requiring accessing to SCI will be submitted to SMC/INS through the Contract Monitor. Upon receipt of a completed background investigation the CSSO will submit a request for SCI eligibility to SMC/INS in accordance with AFMAN 14-304. Contract employees sponsored by other Agencies/Organization shall be certified to SMC/INS through the Servicing SSO for access to SMC Programs. The contractor shall establish and maintain a current billet roster indicating access of SCI personnel on this contract. A copy of this list shall be provided to SMC/INS through the Contract Monitor annually, or as changes occur. The contractor shall also advise SMC/INS through the Contract Monitor immediately upon the reassignment of personnel to duties not associated with this contract, to include termination.

#### **c. Document Control**

SCI furnished in support of this contract remains the property of the SMC Program Office releasing it. The contractor shall maintain an active accountability of all SCI material received, produced, maintained, and disposed of that is in their custody. Upon completion or cancellation of this contract, SCI data will be returned to the custody of the government (Program Office) unless a follow-on contract specifies that material will be transferred to that contract. Inventories of SCI material will be conducted in accordance with DOD 5105.21-M-1 and AFMAN 14-304. Any

supplemental instructions will be furnished and/or made available to the contractor through the Contract Monitor by the User Agency Special Security Office (SMC/INS)

**d. Release of Information**

SCI will be released to contractors only when originator approval has been obtained. The contractor may release such material to any contractor employee assigned to a billet and indoctrinated for Program SCI access under this contract and only when a need-to-know exists. The contractor may release such material to any Special Security Office personnel assigned to HQ SMC, HQ Air Force Space Command (AFSPC), HQ USAF, or DIA upon demand. The contractor shall not release this material to other contractors, subcontract

Federal Government agency employees unless the Program Office, Contract Monitor SMC/INS has granted prior written approval. An access certification to an SMC contractor occupied SCIF does not constitute approval to release SMC contractual material to other contractors, subcontractors, or federal government employees: SMC/INS or Contract Monitor approval is required. SCI will not be released to non-U.S. citizens. SMC/INS approval of an SMC contractor visit certification or permanent certification to another facility will constitute approval to discuss contractual information/material at the facility to be visited.

**e. Reproduction of SCI Information**

The contractor may reproduce any SCI related to this contract at the discretion of the Contract Special Security Officer (CSSO), as long as the copies are controlled in the same way as the originals and they remain in the SCIF. No copies of SCI documents will be transferred to other contractors.

**f. Sub-Contracting**

A CSSO shall coordinate with the Contract Monitor and obtain the concurrence of SMC/INS prior to subcontracting any portion of SCI efforts involved in this contract.

**g. Public Release**

The contractor shall not make references to SCI even by unclassified acronyms, in advertising, promotional efforts, or recruitment for employees.

**h. Block 10k: Other: Automated Information Systems**

Comply with DCID 6/3, DOD 5105.21-M1 Chapters 7 and 8, JDCSISS Current Version, Plan, Concept of Operations and an AIS Security Operations Procedure/Standard Practice Procedure.

**i. Block 11i: TEMPEST Requirements**

TEMPEST security measures must be considered if electronic processing of SCI is involved in accordance with DOD 5105.21-M1 Chapter 7 and Appendix J; AFMAN 14-304, Chapter 7

**j. Block 11k: Defense Courier Service**

This contract requires the use of the Defense Courier Service (DCS). The CSSO will prepare and submit DCS Form 10 in original triplicate to SSO SMC/INS for validation prior to their submittal to the appropriate DCS station (reference to Block 11k).

**k. Block 14: Additional Security Requirements**

The following Directives, Manuals, Instructions, Handbooks, or Pamphlets are incorporated into this contract as they pertain to the access, handling, control, dissemination, processing of Sensitive Compartmented Information:

DCID 6/3  
DCID 6/4  
DCID 6/9  
DOD 5105.21-M1  
JDCSISS  
AFMAN 14-304

**l. Block 15: Inspections**

Defense Security Service is relived of inspection responsibilities pertaining to Sensitive Compartmented Information associated with this contract. The following activity is designated as inspection authority and the User Agency SSO for SCI requirements in accordance with DOD 5105.21-M-1, and AFMAN 14-304.

SMC/INS (SMC SSO)  
483 North Aviation Boulevard  
Los Angeles AFB  
El Segundo, CA 90245-2808

The User Agency Special Security Officer (SSO) is:

SMC/INS  
(310) 653-4122

The Alternate Special Security Officer (ASSO) is:

SMC/INS  
(310) 653- 4508

The contractor will handle all SCI and non-SCI intelligence information in accordance with the markings and restrictive caveats. All security classification guidance will be derived from source documents. Additional security classification guidance, if required, will be obtained from the source of the SCI information.

**(2) Non-SCI**

Provisions for the handling of Non-SCI or "Collateral" Intelligence by contractors is governed by Chapter 9, Section 3 of DoD 5220.22-M, the National Industrial Security Program Operating



Manual, 2006 (NISPOM). Particular emphasis is placed on the contractor(s) correctly understanding and heeding intelligence portion markings.

As classified material, collateral intelligence will be afforded the same protections, safeguards and precautions required by any classified material unless special intelligence related handling instructions are additionally imposed. These basic safeguards are found in DoD 5200.1-R, Information Security Program and AFI 31-401, Information Security Program Management. The disclosure or release of intelligence derived information, whether its status is collateral or SCI, is not authorized without the prior consent of SMC/IN.

#### **Reference Block 10j: For Official Use Only (FOUO) Handling Instructions**

FOR OFFICIAL USE ONLY (FOUO) information will be handled as follows:

1. Description. "For Official Use Only (FOUO)" is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The FOIA specifies nine exemptions that may qualify certain information to be withheld from release to the public, if, by its disclosure, a foreseeable harm would occur. They are:

- a. Information that is currently and properly classified.
- b. Information that pertains solely to the internal rules and practices of the Agency. (This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an Agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)
- c. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
- d. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the Government's ability to obtain like information in the future, or protect the Government's interest in compliance with program effectiveness.
- e. Inter-Agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.
- f. Information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

g. Records or information compiled for law enforcement purposes that:

- (1) Could reasonably be expected to interfere with law enforcement proceedings;
- (2) Would deprive a person of a right to a fair trial or impartial adjudication;
- (3) Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others;
- (4) Disclose the identity of a confidential source;
- (5) Disclose investigative techniques and procedures; or
- (6) Could reasonably be expected to endanger the life or physical safety of any individual.

h. Certain records of agencies responsible for supervision of financial institutions.

i. Geological and geophysical information concerning wells.

## 2. General.

a. Information that is currently and properly classified shall be withheld from mandatory release under the first exemption of the Freedom of Information Act FOIA. "FOR OFFICIAL USE ONLY" (FOUO) is applied to information that may be exempt under one or more of the other eight exemptions. So, by definition, information shall be unclassified in order to be designated FOUO. If an item of classified information is declassified, it may be designated FOUO if it qualifies under one of the other exemptions of the FOIA. This means that:

- (1) Information cannot be classified and FOUO at the same time. Therefore, classified documents containing FOUO information cannot bear an overall document marking of FOUO. However, portions or pages of a classified document, that contain only FOUO information will be marked as FOUO.
- (2) Information that is declassified may be designated FOUO, only if it is believed to fit into one or more of the last eight exemptions (exemptions 2 through 9).

b. The FOIA provides that, for information to be exempt from mandatory release, it must fit into one of the qualifying categories and there must be a legitimate Government purpose served by withholding it. Simply because information is marked FOUO does not mean it automatically qualifies for exemption. If a request for a record is received, the information must be reviewed to see if it meets this dual test. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released. Some types of

records (for example, personnel records) are not normally marked FOUO, but may still qualify for withholding under FOIA.

### 3. Marking.

a. Marking information FOUO does not automatically qualify it for exemption. If a request for a record is received, the information shall be reviewed to determine if it actually qualifies for exemption. Similarly, the absence of the FOUO marking does not automatically mean the information shall be released. Some types of records (for example, personnel records) are not normally marked FOUO, but may still be withheld under the FOIA. All DoD unclassified information must be reviewed before it is released to the public or to foreign governments and international organizations.

b. Information that has been determined to qualify for FOUO status should be indicated by markings when included in documents and similar material. Markings should be applied at the time documents are drafted, whenever possible, to promote proper protection of the information.

(1) Unclassified documents and material containing FOUO information shall be marked as follows:

- a. Documents will be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one).
- b. Pages of the document that contain FOUO information shall be marked "FOR OFFICIAL USE ONLY" at the bottom.
- c. Portion Marking FOUO Information. Subjects, titles and each section, part, paragraph, and similar portion of an FOUO document shall be marked to show that they contain information requiring protection. Use the parenthetical notation "(FOUO)" to identify information as For Official Use Only for this purpose. Place this notation immediately before the text.
- d. Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings that alert the holder or viewer that the material contains FOUO information.
- e. FOUO documents and material transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

"This document contains information exempt from mandatory disclosure under the FOIA. Exemption(s) \_\_\_\_\_ apply."

- (2) Classified documents and material containing FOUO information shall be marked as required by Chapter 4 of the NISPOM (or DoD 5200.1-R, Chapter 5, as applicable), with FOUO information identified as follows:
    - a. Overall markings on the document shall follow the rules in NSPOM Chapter 4 (or DoD 5200.1-R, Chapter 5). No special markings are required on the face of the document because it contains FOUO information.
    - b. Portions of the document shall be marked with their classification as required by NISPOM Chapter 4 (or DoD 5200.1-R, Chapter 5). If there are unclassified portions that contain FOUO information, they shall be marked with "FOUO" in parentheses at the beginning of the portion. Since FOUO information is, by definition, unclassified, the "FOUO" is an acceptable substitute for the normal "U."
    - c. Pages of the document that contain classified information shall be marked as required by NISPOM Chapter 4 (or DoD 5200.1-R, Chapter 5). Pages that contain FOUO information but no classified information will be marked "FOR OFFICIAL USE ONLY" at the top and bottom.
  - (3) Transmittal documents that have no classified material attached, but do have FOUO attachments shall be marked with a statement similar to this one:

"FOR OFFICIAL USE ONLY ATTACHMENT."
  - (4) Each part of electrically transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text.
4. Access to FOUO Information.
- a. No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose.
  - b. The final responsibility for determining whether an individual has a valid need for access to information designated as FOUO rests with the individual who has authorized possession, knowledge or control of the information and not on the prospective recipient.
  - c. Information designated as FOUO may be disseminated within the DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to

conduct official business for the Department of Defense, provided that dissemination is not further controlled by a Distribution Statement.

- d. DoD holders of information designated as FOUO are authorized to convey such information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a government function. If the information is covered by the Privacy Act, disclosure is only authorized if the requirements of DoD 5400.11-R are satisfied.
- e. Release of FOUO information to Congress is governed by DoD Directive 5400.4. If the information is covered by the Privacy Act, disclosure is authorized if the requirements of DoD 5400.11-R are also satisfied.
- f. DoD Directive 7650.1 governs release of FOUO information to the General Accounting Office (GAO). If the information is covered by the Privacy Act, disclosure is authorized if the requirements of DoD 5400.11-R are also satisfied.

#### 5. Protection of FOUO Information

- a. During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. After working hours, store FOUO information in unlocked containers, desks or cabinets if Government or Government-contract building security is provided. If such building security is not provided, store the information in locked desks, file cabinets, bookcases, locked rooms, etc.
  - b. FOUO information and material may be transmitted via first class mail, parcel post or, for bulk shipments, via fourth class mail. Electronic transmission of FOUO information, e.g., voice, data or facsimile, e-mail, shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI), whenever practical.
  - c. FOUO information may only be posted to DoD Web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum dated December 1998, Subject: "Web Site Administration".
  - d. Record copies of FOUO documents shall be disposed of according to the Federal Records Act and the DoD Component records management directives. Non-record FOUO documents may be destroyed by any of the means approved for the destruction of classified information, or by any other means that would make it difficult to recognize or reconstruct the information.
6. Unauthorized Disclosure. The unauthorized disclosure of FOUO does not constitute an unauthorized disclosure of DoD information classified for security purposes. However, appropriate administrative action shall be taken to fix responsibility for unauthorized disclosure

of FOUO whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The Military Department or other DoD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

#### **Reference Block 10k: Other**

Commercially Hosted IR Payload (CHIRP) data collected within the Mission Operations Center shall not be disseminated to any other entities other than the Mission Analysis Center and government authorized points of presence (e.g. the Aerospace Fusion Center or the Aerospace Research Center) without express permission from the 3GIRS program office.

#### **Reference Block 11d: Fabricate, Modify, Or Store Classified Hardware**

The Contractor is required to provide adequate storage to the level of *SECRET* for classified hardware that, due to size or quantity, cannot otherwise be safeguarded in GSA approved storage containers.

#### **Reference Block 11f: Access to Classified Information Outside The US**

Contractor requires access to U.S. Classified Information outside the U.S. Possession and Trust Territories.

The User Agency (HQ, Space and Missile Systems Center) will furnish complete classification guidance for the service to be performed. The highest level of classification for the contract is **Top Secret**.

All other foreign disclosure is covered by AFI 16-201, and Delegated Disclosures Letters provided by SMC/PIP. A training program must be developed to insure personnel are aware of foreign disclosure guidelines.

#### **Reference Block 11g: Be Authorized To Use The Services of Defense Technical Information Center (DTIC) Or Other Secondary Distribution Center**

The contractor may access information provided by DTIC by complying with all established safeguards and following the registration procedures as set forth in Chapter 11 Section 2 of the NISPOM (DoD 5220.22M).

#### **Reference Block 11i: TEMPEST Requirements**

TEMPEST security measures must be considered if electronic processing of classified information is involved in accordance with DoD 5105.21-M-1, Chapter 7 and Appendix I, and AFMAN 14-304, Chapter 7.

This contract requires electronic processing of classified information and will be permitted only after EMSEC requirements are met as specified in the following EMSEC guidance:

## **61 CS/SCBS EMSEC REQUIREMENTS FOR SYSTEMS PROCESSING CLASSIFIED NATIONAL SECURITY INFORMATION**

The following guidance outlines Emission Security (EMSEC) requirements that government contractors must comply with prior to processing classified data. These requirements are established for processing DoD SECRET information, but higher than DoD SECRET may call for more stringent requirements.

The contractor shall ensure that EMSEC conditions related to this contract are minimized and that Red/Black Separation Requirements are implemented in accordance with Attachment 1.

### **EMSEC Red/Black Requirements**

**Countermeasure Application:** These paragraphs discuss how to apply Red/Black Separation countermeasures and under what conditions they would not be required.

#### **Keep RED and BLACK Signal Lines Separated.**

Keeping RED signal lines about 6 inches away from BLACK signal lines will reduce coupling to a level low enough to prevent detection at great distances (over one mile). This separation may be reduced to two inches if the RED signal lines are shielded.

#### **Keep RED Signal Lines Separated from BLACK Power Lines.**

Keeping RED signal lines about 6 inches away from BLACK power lines will reduce coupling to a level low enough to prevent detection at great distances (over one mile). This separation may be reduced to two inches if the RED signal lines are shielded.

#### **Keep RED Processors Separated from BLACK Telephones and Telephone Lines.**

Keep non-EMSEC-approved printers at least 3 feet away from telephones. Do not use the telephone while printing classified information. Keep all non-EMSEC-approved equipment at least 3 feet away from telephone lines; two inches if the telephone lines are shielded.

### **EMSEC SEPARATION MATRIX**

This matrix applies to the processing of Collateral Secret Information.

RED \ BLACK	Crypto Equipment	Unshielded Signal And Telephone Lines	Shielded Telephone Lines	Power Lines
Crypto Equipment	0	3 Feet	2 Inches	2 Inches
Unshielded Signal Lines	6 Inches	6 Inches	2 Inches	6 Inches
Shielded Signal Lines	2 Inches	2 Inches	2 Inches	2 Inches
EMSEC Approved	2 Inches	6 Inches	2 Inches	None

Equipment				
Non-EMSEC Approved Equipment	3 Feet	3 Feet	2 Inches	None

## **SPECIAL ITEM EMISSION REQUIREMENTS**

**Special Items.** People may innocently introduce other radio devices, such as pagers, hand-held portable transceiver radios, cellular telephones, cordless telephones, and cordless microphones into the area processing classified national security information with disastrous results. Also, alarm systems may use radio transmitters to alert remotely located security or fire-fighting teams.

**Hand-Held Radios.** Hand-held radio transceivers used with intrabase radios (sometimes abbreviated IBR) and land mobile radios (sometimes abbreviated LMR) deserve special consideration because of their unique operational applications. A person may carry these devices into an area where classified national security information is processed. If the person is carrying such a device works in a facility and works near computer systems processing classified information, that person should either turn off the device and use the telephone or keep the device 2 meters from classified processors. No transmissions are allowed near classified processors when they are in operation. If the person carrying the device is a short-term visitor, it may not be necessary to turn off the radio if the visitor is moving about in the facility. However, transmissions near classified processors must be avoided.

**Beepers and Pagers.** Beepers and pagers deserve special consideration because of their unique operational applications. A person may carry these devices into an area near processors where classified national security information is being processed. If the person is carrying such a device works in the facility and works near computer systems processing classified information, that person should either turn off the pager device and use the telephone or keep the device 2 meters from classified processors. If the person carrying the device is a short-term visitor, it may not necessary to turn off the device if the visitor is moving about in the facility. If the pager device has a transmit capability, follow the instructions for hand-held radios.

**Alarm Systems.** The mode of operation of alarm systems radio frequency transmitters will determine their treatment. Any such transmitter with a continuous transmit mode or a high duty cycle (transmits most of the time) must meet the same separation requirements as all other transmitters (See para. 1.1). If they do not meet these requirements, exclude them from operating in the vicinity of computer systems processing classified national security information. Low duty cycle (transmits short bursts infrequently) systems are not considered hazards and require no special treatment.

**Cellular Telephones.** When a cellular telephone is used as an operational necessity, separate it at least 5 meters from RED processing equipment. If a cellular telephone is personal property, it's use near computer systems processing classified national security information is prohibited. Disable cellular telephones from receiving calls or separate them 10 meters from RED processing equipment.

**Cordless Telephones.** When a radio frequency cordless telephone is used as an operational necessity, separate it 5 meters from RED processing equipment. When the cordless telephone is personal property, it's use near computer systems processing classified national security information is prohibited. Disable personal cordless telephones from receiving calls or separate them 10 meters from RED processing equipment. There are no separation requirements for infrared cordless telephones.

**Cordless Microphones.**



**Radio Frequency Cordless Microphones.** When a radio frequency cordless microphone, encrypted or unencrypted, is used for broadcasting either classified national security information or unclassified information, separate it 10 meters from RED processing equipment. Use of unencrypted radio frequency cordless microphones for classified broadcasts is prohibited.

**Infrared Cordless Microphones.** Use of infrared cordless microphones for broadcasting classified national security information is permitted in suitably constructed and approved rooms. During classified use, doors to approved areas should be kept closed and windows should be covered with drapes or blinds.

**Cordless Keyboards.** When a radio frequency cordless keyboard is used, separate it 10 meters from RED processing equipment. Radio frequency cordless keyboards cannot be used to process classified national security information unless encrypted.

**Wireless Local Area Networks.** When a radio frequency wireless local area network is used, separate the transmitter and receiver units 10 meters from RED processing equipment.

#### **Reference Block 11j: OPSEC**

Contractor will comply with all Program Protection Plans/Security Classification/ Declassification Guide specified in the applicable Delivery Order Statement of Work or the DD Form 254. The contractor will accomplish the following minimum requirements in support of the User Agency Operations Security (OPSEC) Program and protect OPSEC Critical Information. Items of Critical Information are those facts which individually or in the aggregate reveal sensitive details about SMC programs and contractor operations, and thus require protection from adversarial collection or exploitation.

Protect Critical Information and activities which could compromise classified information or operations, or degrade the planning and execution of military operations performed by the contractor in support of the mission. Such information may be marked FOR OFFICIAL USE ONLY, Privacy Act of 1974, COMPANY PROPRIETARY, Export Controlled, or otherwise designated as sensitive by the Special Program Office or SMC/PIP (OPSEC Manager).

Review items on the critical information list (CIL) as contained within the SMC OPSEC Plan and determine applicable to contractor operations. Include OPSEC as a part of the contracts ongoing security awareness program conducted in accordance with Chapter 3, Section 1, of the NISPOM or Chapter 3 of AFI 10-701, as applicable. Be responsive to the SMC OPSEC Program Manager on a non-interference basis.

#### **Reference Block 11k: Defense Courier Service**

Use of Defense Courier Service for the required COMSEC account is authorized. The Contractor Special Security Officer (CSSO) will prepare and submit DCS Form 10 in original triplicate to the program SSO for validation prior to their submittal to the appropriate DCS station.

## **Block 11.1 Export Control Requirements**

### **A. Technology Transfer and Information Control**

1.0 **General.** The requirement of Paragraph B 1.0 General below shall apply.

2.0 **Markings.** The requirement of Paragraph B 2.0 *Markings* below shall apply.

### **B. Arms Export Control Act**

1.0 **General.** Certain contract deliverables, corresponding with CHIRP objectives are determined to meet the criteria of the International Traffic in Arms Regulation (ITAR) of the Arms Export Control Act. Certain CHIRP deliverables meet the criteria of Category XV *Spacecraft Systems and Associated Equipment* of the U.S. Munitions List (USML). Specifically deliverables meet the USML, Category XV at:

- Paragraphs (a) and (e): prototype and qualification AIRSS/3GIRS components, and
- Paragraphs (a) and (f): technical data to include design, development, or manufacturing data

These items are specifically designed components for the AIRSS/3GIRS constellation.

2.0 **Markings.** The cover or the first page of unclassified documents containing AIRSS/3GIRS design, development, or manufacturing data shall contain the following statement:

**WARNING -This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C. 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401, et seq. Violation of these export-control laws is subject to severe criminal penalties. Dissemination of this document is controlled under DoD Directive 5230.25 and AFI 61-204.**

3.0 **Unauthorized Disclosure.** Government and contractor personnel must act to protect AIRSS/3GIRS design, development, and manufacturing data under their control from unauthorized disclosure to any foreign person or a U.S. person residing in a foreign country. Government and contractor organizations must inform The U.S. State Department under the provision of the ITAR regarding any unauthorized disclosures of the 3GIRS data list above, in support of this contract.

4.0 **Authorized Disclosure.** The Contractor shall comply with the provisions of the ITAR regarding the export of 3GIRS prototype hardware or 3GIRS qualification hardware or 3GIRS design, development, or manufacturing data. The 3GIRS program office will comply with the provisions of Air Force Instruction 16-201 *Air Force Foreign Disclosure and Technology Transfer* regarding the disclosure of said 3GIRS data to foreign representatives.

## **Reference Block 12: Release of Information**

The contractor shall refer to the appropriate Program Protection Plan/SCG for procedures regarding the release of program information to the general public and to US citizens. Release of information must be approved by SMC/PA.

### **Reference Block 13: Security Guidance**

The contractor shall protect critical program information, technologies, and systems (CPI), and critical system resource (CSR), as identified in Program Protection Plan and as identified in the contractor's Program Protection Implementation Plan, as approved by the 3GIRS program office. The security classification guides (SCG) are meant to be integrated into the broader scope of a PPP. The prime contractor shall develop a PPIP to implement the protection of critical program information, technologies, and systems (CPI), and critical system resource (CSR). The prime contractor will flow-down applicable CPI and CSR to any subcontractor with protection requirements as identified in its PPIP. Additionally, classified national security information, special access and unclassified controlled information as prescribed in applicable security classification guides will be protected as outlined in the NISPOM.

Refer to the Technical Assessment Control Plan (TA/CP) for release to foreign entities or foreign nationals residing in foreign countries; or to press media must coordinate through SMC/PIP Foreign Disclosure Office.

**The contractor shall comply with the general security provisions of the following documents, including changes or revisions:**

1. DCID 6/3, Protection Sensitive Compartmented Information Within Information System, 05 Jun 1999
2. DCID 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI) , 2 July 1998 (replaced DCID 1/14)
3. DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities, 18 November 2002
4. DoD 5400.7-R/AF Sup, 24 June 2002, DoD Freedom Of Information Act Program
5. DIAM 50-4, 30 Apr 97, DoD Intelligence Information Systems (DoDIIS) Information Systems Security Program
6. DoD 5220.22-M, Revision 1, 1 April 2004, Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement
7. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) and subsequent changes or revisions

8. DoD 5220.22-M-Sup, Sep2004, National Industrial Security Program Operating Manual (NISPOM)
9. DoD 5105.21-M-1, 3 Aug 98, Sensitive Compartmented Information Administrative Security Manual
10. DoDD 5200.39, 10 Sept 97, Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection.
11. AFI 14-302, 18 Jan 94, Control, Protection, and Dissemination of Sensitive Compartmented Information.
12. AFI 14-303, 1 Apr 99, Release of Intelligence to U.S. Contractors.
13. The Contractor shall comply with AIRSS/3GIRS Security Classification Guide (SCG), 24 July 2006, FOUO; including changes or revisions.
14. The Contractor will comply with the SMC and/or the SMC/XR OPSEC plan 10-100, 19 Feb 03 and/or the SMC OPSEC Plan July 2004.